

Standards

The standards landscape, with a focus on standards related to secure identity credentials and interoperability.

Presented to the State of California

Teresa Schwarzhoff

*Computer Security Division
Information Technology Laboratory*

Topics

Types of standards and U.S. strategy

Standards development organizations

Organizations of interest

Emerging interoperability standard

Innovation, security, and standards

Telegraph, Telephone, Internet, World Wide Web

- *new communication*
- *new computer technologies*
- *new business opportunities*
- *new forms of crime*

As the scale for innovation increases

- *the assurance on identity decreases (all things equal)*
- *security mechanisms decay*
- *standardization becomes increasingly important*

Perspective

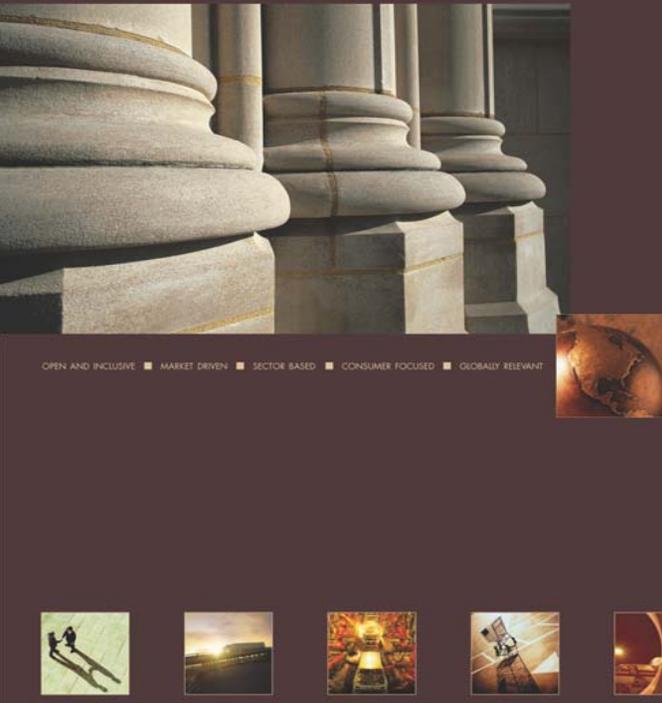
Technologies need standards.

Interoperability based on standards.

Cyber security requires standards.

Homeland security requires international cyber security standards.

International, interoperable standards should be the strategic goal.



OPEN AND INCLUSIVE ■ MARKET DRIVEN ■ SECTOR BASED ■ CONSUMER FOCUSED ■ GLOBALLY RELEVANT

- 1 – Strengthen participation by government in development and use of **voluntary consensus standards** through public/private partnerships
- 2 – Continue to address the environment, health, and safety in the development of **voluntary consensus standards**
- 3 – Improve the responsiveness of the standards system to the views and needs of consumers
- 4 – Actively promote the consistent worldwide application of internationally recognized principles in the development of standards.
- 5 – Encourage common governmental approaches to the use of voluntary consensus standards as tools for meeting regulatory needs
- 6 – Work to prevent standards and their application from becoming technical trade barriers to U.S. products and services
- 7 – Strengthen international outreach programs to promote understanding of how **voluntary, consensus-based**, market-driven sectoral standards can benefit businesses, consumers and society as a whole
- 8 – Continue to improve the process and tools for the efficient and timely development and distribution of **voluntary consensus standards**
- 9 – Promote cooperation and coherence within the U.S. standards system
- 10 – Establish standards education as a high priority within the United States private, public and academic sectors
- 11 – Maintain stable funding models for the U.S. standardization system
- 12 – Address the need for standards in support of emerging national priorities

“United States Standards Strategy establishes a framework that can be used to ... enhance consumer health and safety, ..., and ... advance U.S. viewpoints in the regional and international arena.”

http://www.ansi.org/standards_activities/nss/usss.aspx?menuid=3

The United States standards strategy is framed by the use of *national and international consensus based voluntary standards.*

Standards development

Participation in the process

Which ones?

How?

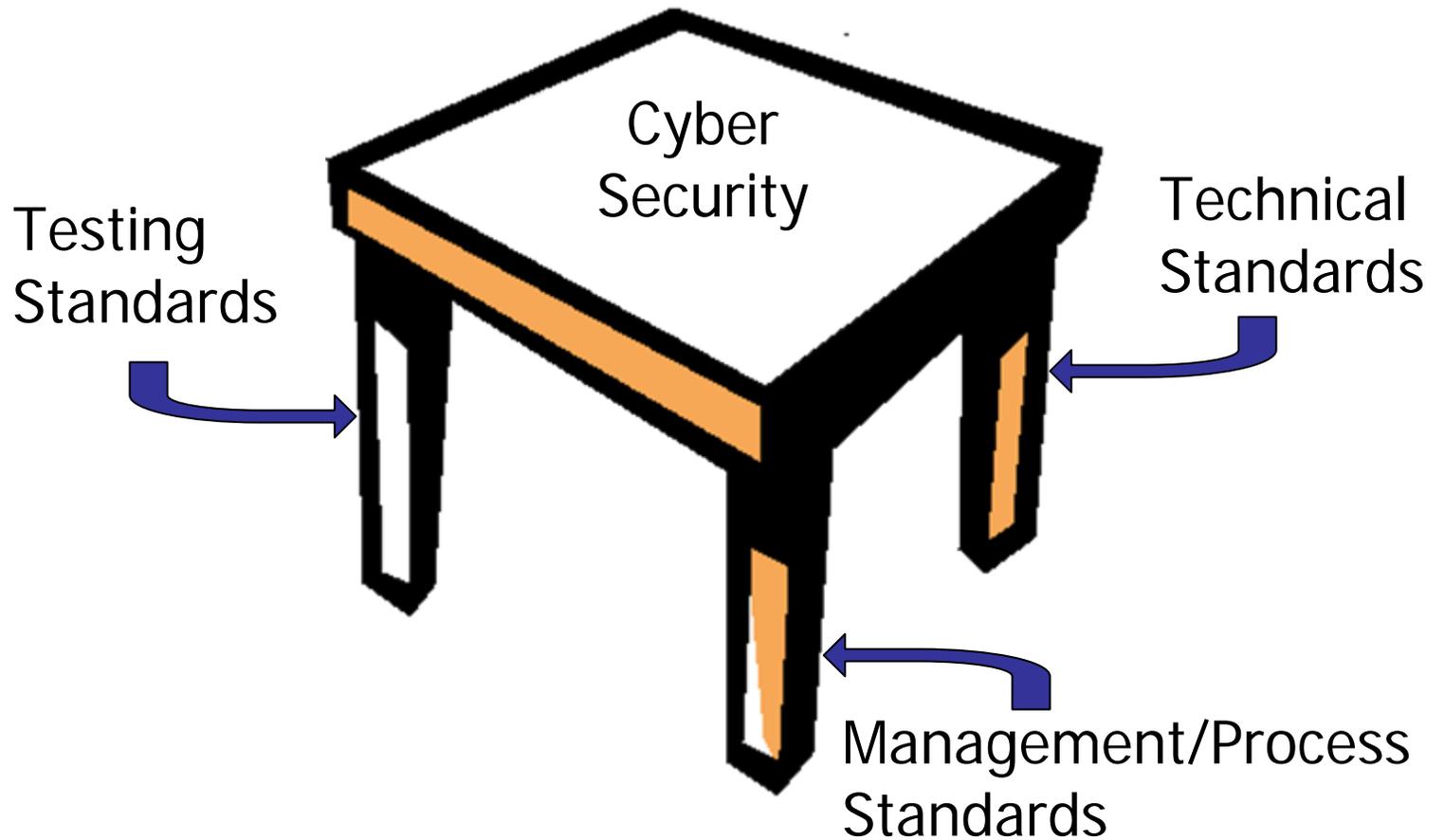
Why?

Types of standards

- Open
- Proprietary
- Federal
- International, Regional, National, Company
- Voluntary Consensus, De Facto
- Consortia)

Preference is open, international, voluntary consensus standards.

Three Categories of Cyber Security Standards



Examples of Management/Process Standards

ISO/IEC TR 13335 *Guidelines for the Management of IT Security (GMITS)* (multiple parts)

ISO/IEC 17799:2000, *Code of Practice for Information Security Management Systems*

FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*

NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*

Examples of Testing Standards

Cryptographic Module Validation Program
(CMVP)

FIPS 201 PIV card application and
middleware

Examples of Technical Standards

FIPS 197-2001 *Advanced Encryption Standard (AES)*
(ISO/IEC 18033-3)

ISO/IEC 15408:1999 *Common Criteria for IT Security
Evaluation* (three parts)

FIPS 201 – Personal Identity Verification

ANSI INCITS 358: 2002 *BioAPI Specification*

ISO/IEC 24727:2008 Integrated card circuit application
programming interfaces (six parts)

Some terms and clarifications

SDO – standards development organization

U.S. TAG - the U.S. SDO designated as the **technical advisory group** for an international SDO

Technical committee (international) versus Sub committee (national)

Work group (international) versus Task Group (national)

ANSI's role is to accredit SDOs

InterNational Committee for Information Technology Standards (INCITS)

INCITS is the primary U.S. focus of standardization in the field of Information and Communications Technologies (ICT) encompassing storage, processing, transfer, display, security, management, organization, and retrieval of information.

INCITS serves as ANSI's designated US Technical Advisory Group for ISO/IEC Joint Technical Committee 1.

<http://www.incits.org/>

Developers of Standards

National Institute of Standards and Technology

ISO/IEC JTC 1 on Information Technology*

ISO TC 68 on Banking and Other Financial Services

Internet Engineering Task Force (IETF)

InterNational Committee for Information Technology Standards (INCITS)*

X9, Inc. - Financial Industry Standards

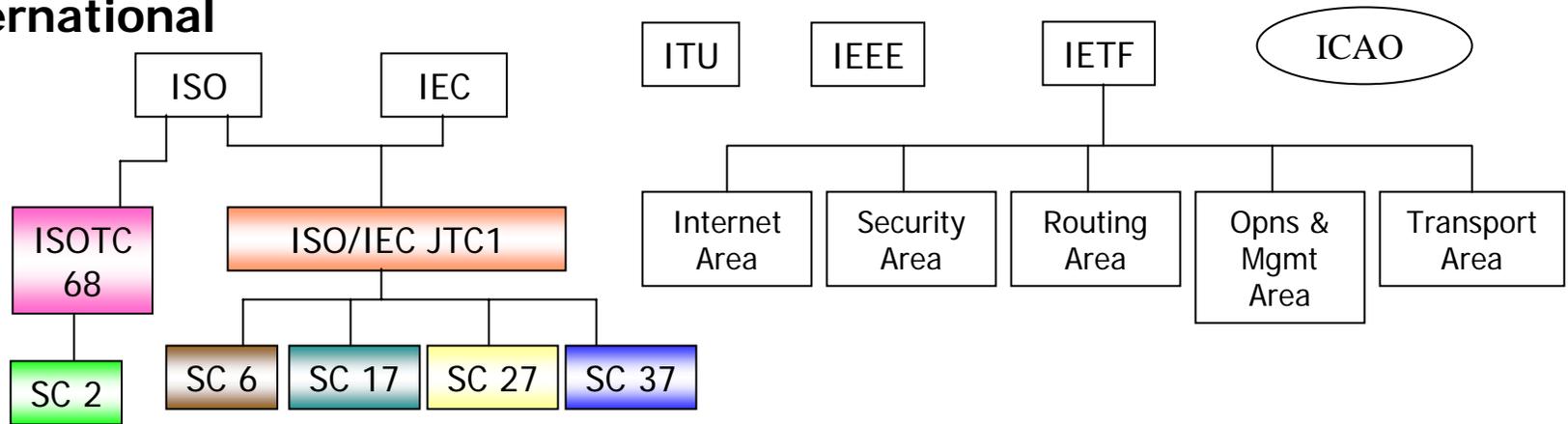
Institute of Electrical and Electronic Engineers (IEEE)

Many Others

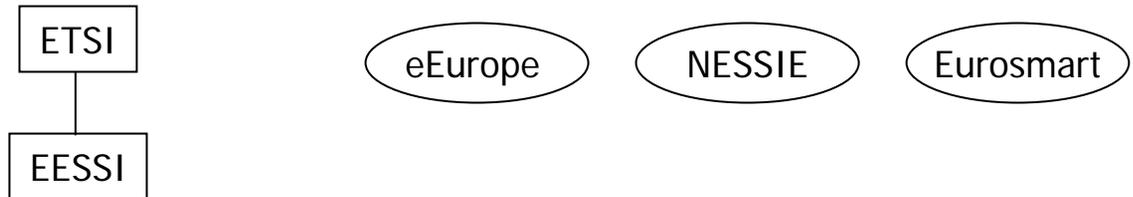
* Where most of IT and identity standards happen.

Relevant standards activities

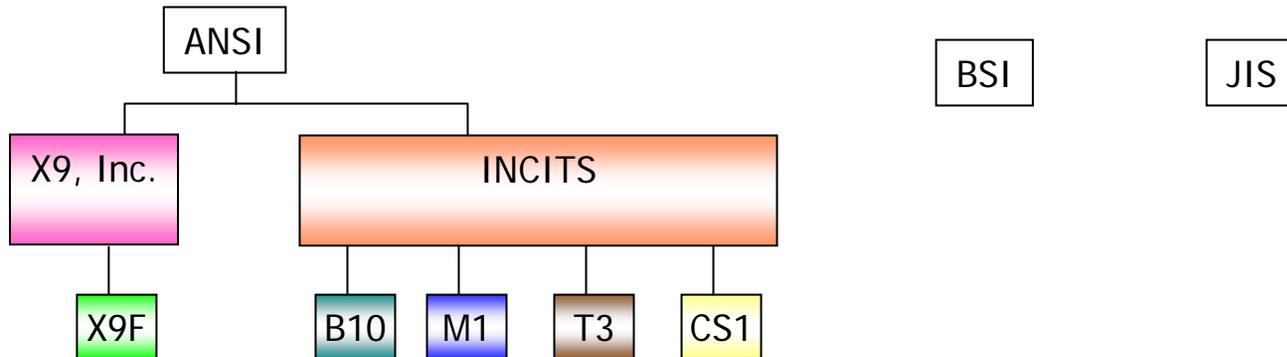
International



Regional



National



Relevant ISO/IEC JTC 1 sub-committees and the U.S. technical advisory group

SC 6 – Telecommunications and exchange between systems

SC 17 – Cards and personal identification

SC 27 – Security techniques

SC 37 - Biometrics

US TAGS:

T3 – Open Distributed Processing

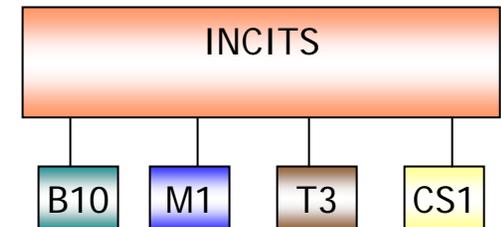
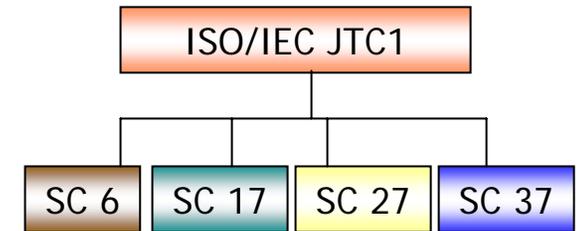
B10 – Identification Cards and Related Devices

CS1 – Cyber Security

M1 – Biometrics

ISO URL:

<http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/customview.html?func=ll&objid=327993>



SC 37 work groups

- WG 1 Harmonized biometric vocabulary
- WG 2 Biometric technical interfaces
- WG 3 Biometric data interchange formats
- WG 4 Biometric functional architecture and related profiles
- WG 5 Biometric testing and reporting
- WG 6 Cross-Jurisdictional and Societal Aspects of Biometrics

<http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/customview.html?func=ll&objId=327993>

SC 17 work groups

WG1 - PHYSICAL CHARACTERISTICS AND TEST METHODS FOR IDENTIFICATION CARDS

Physical characteristics, embossing, magnetic stripe, and test methods for conformance and card durability.

WG3 - MACHINE READABLE TRAVEL DOCUMENTS

To prepare a revised text of ISO 7501; monitor the standards referenced; consider and define standards for machine readable travel documents and related machine readable cards (see Recommendation 3 of N 379); co-ordination of JTC1 liaison with ICAO for maintenance of ICAO 9303, machine readable passports and related ICAO documents.

WG4 - INTEGRATED CIRCUIT CARDS WITH CONTACTS

To define specifications related to the Integrated Circuits Card with Contacts within the area of SC17.

WG5 - REGISTRATION MANAGEMENT GROUP

To serve as the RMG for ISO/IEC 7812 Parts 1 & 2 and ISO/IEC 7816-5. Responsibility for maintenance of ISO/IEC 7812 Parts 1 & 2. Responsible for Registration of Application providers under ISO/IEC 7816-5. To liaise, when necessary with Working Group 4 on matters relating to ISO/IEC 7816-5.

WG7 - FINANCIAL TRANSACTION CARDS THIS WORKING GROUP HAS BEEN STOOD DOWN

To revise ISO/IEC 7813 and its amendment 1 in accordance with SC17 resolution 365 and to carry out any further revisions as necessary.

WG8 - CONTACTLESS INTEGRATED CIRCUIT(S) CARDS, RELATED DEVICES AND INTERFACES

The scope of WG8 is to develop standards for the Contactless Integrated Circuit(s) Card which do not preclude the incorporation of other Standard technologies on the card.

WG9 - OPTICAL MEMORY CARDS AND DEVICES

Enhanced OMC technologies enabling more data capacity, fast access and high reliability based on existing standard technologies or new technologies. Software or programming interface for accessing OMC data contents. (Host application program will be able to use this interface for easier implementation. Access method software of OMCs application program.) Physical assignment and /or logical assignment for OMC media use. Logical data structures in OMCs data (file structure etc).

WG10 - MOTOR VEHICLE DRIVER LICENCE AND RELATED DOCUMENTS

Draft Terms of Reference: Standardization in the field of Motor vehicle driver licences.

WG11 - Application of Biometrics to Cards and Personal Identification

Interoperability for interindustry and government applications using personal identification technologies, e.g. biometrics. Excludes generic biometrics as undertaken by SC37.

Other standard groups of interest

ISO TC 68 – Financial services

U.S. TAG: X9 – Financial industry standards

ISO TC 215 – Health informatics

U.S. TAG: HIMSS - Healthcare Information and Management Systems Society

ITU-T – Telecommunication

Identity Management Global Standards Initiative

Other initiatives

WHTI – Western Hemisphere Travel Initiative

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), requiring travelers to present a passport or other document denoting identity and citizenship when entering U.S.

http://www.dhs.gov/xprevprot/programs/gc_1200693579776.shtm

Real-ID Act - secure driver license

<http://edocket.access.gpo.gov/2008/08-140.htm>

FRAC – first responder/emergency responder
NIST in discussion with DHS

OSTP, National Science and Technology Council, Committee on Technology
Recent publication on identity management – recommendations for the next administration

<http://www.ostp.gov/cs/nstc>

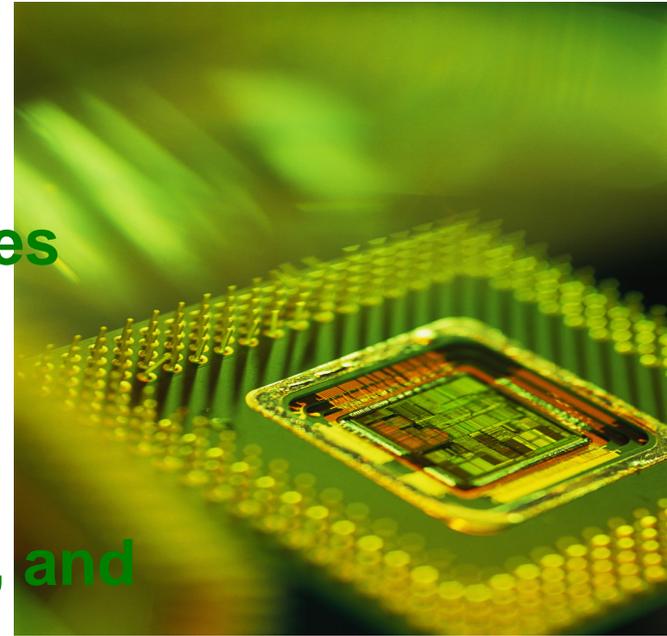
Emerging interoperability standard

**ISO/IEC 24727- Identification Cards -
Integrated circuit cards programming
interfaces**

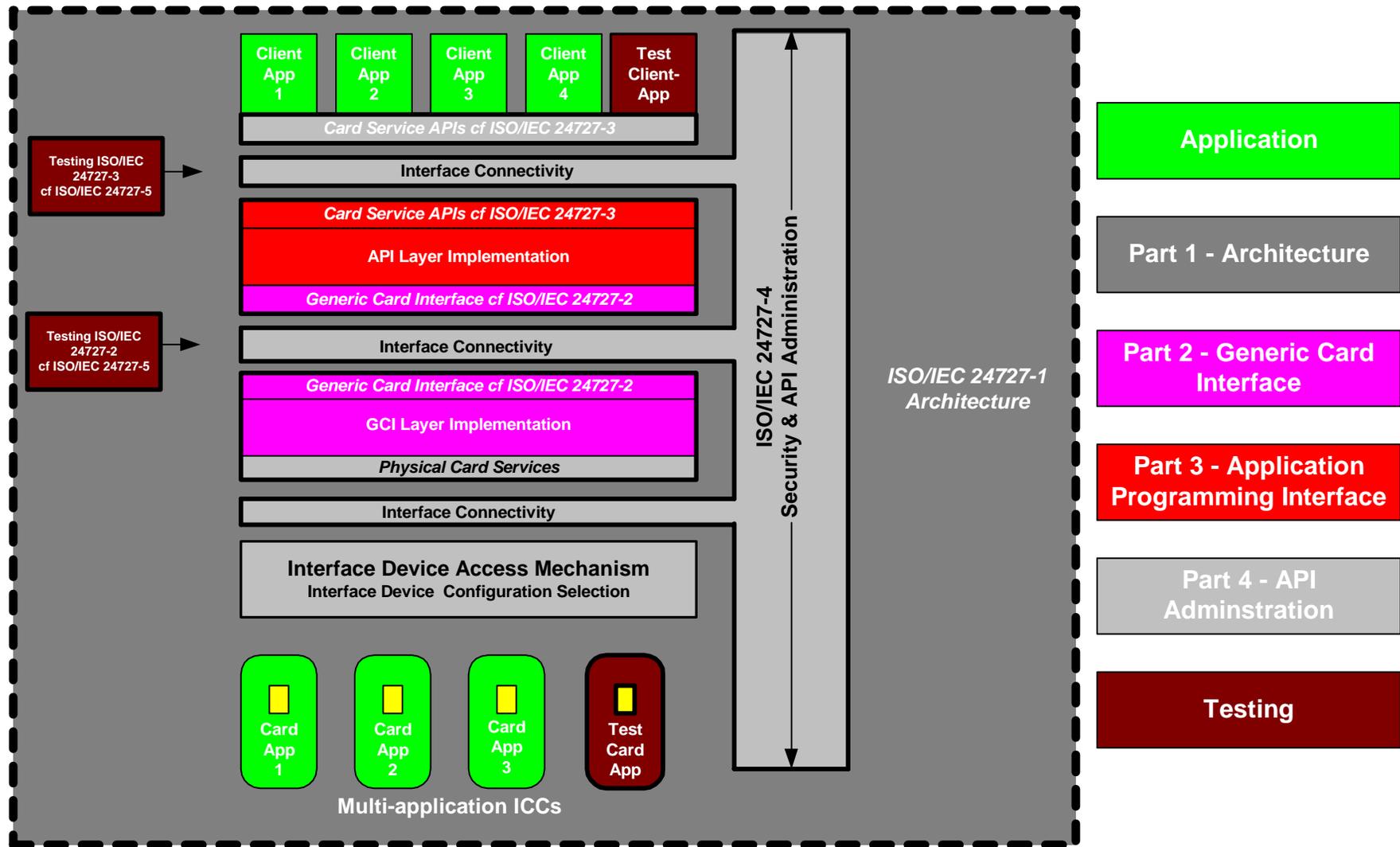
ISO/IEC 24727 multi-part standard

ISO/IEC 24727 – Identification Cards - Integrated circuit cards programming interfaces

- ✓ Builds upon ISO/IEC 7816
 - ✓ **Focuses on services and interfaces**
 - ✓ Card type neutral
 - ✓ Contact and contactless agnostic
 - ✓ **eID: identification, authentication, and signature services**
- ✓✓✓ Goal: Independent implementations that are interchangeable



ISO/IEC 24727 is about interfaces for interoperability.



ISO/IEC 24727-1

ISO/IEC 24727 Identification Cards - Integrated circuit cards programming interfaces – Part 1: Architecture

- Overarching framework
- Common terminology
- Logical architecture for framework

Status

- Published, available for purchase via your national body standards group or the ISO on-line store

ISO/IEC 24727-2

ISO/IEC 24727 Identification Cards - Integrated circuit cards programming interfaces – Part 2: Generic card interface

- Common card interface
- 7816 toolkit fine-tuning
- Discovery mechanism
 - Card capability description (CCD)
 - Application capability description (ACD)
- ISO/IEC 20060
- ISO/IEC 7816-15

Status

- Published

ISO/IEC 24727-3

ISO/IEC 24727 Identification Cards - Integrated circuit cards programming interfaces – Part 3: Application interface

- New territory for smart card standards
- Normative API/middleware
- Normative authentication protocols

Normative Services

- Connection
- Card application discovery and retrieval
- Identity
- Cryptographic
- Authorization

Status

- Soon to be published

Example of actions for a service found in ISO/IEC 24727-3:

Connection service

Initialize

Terminate

CardApplicationPath

CardApplicationConnect

CardApplicationDisconnect

CardApplicationStartSession

CardApplicationEndSession

Authentication protocols

PIN

password

symmetric key

asymmetric key

digital certificate

biometric image or template

pair of symmetric keys; e.g., one for encryption and one for message authentication code (MAC) generation

Name of authentication protocol	General definition of protocol
ASYMMETRIC INTERNAL AUTHENTICATE	Fetch certificate Send challenge to be signed (on-card) Validate (off-card) signature based on certificate
ASYMMETRIC EXTERNAL AUTHENTICATE	Fetch challenge Sign (off-card) and validate signature (on-card)
SYMMETRIC INTERNAL AUTHENTICATE	Send challenge to be signed (on-card) Validate signature (off-card)
SYMMETRIC EXTERNAL AUTHENTICATE	Fetch challenge Sign challenge (off-card) Validate signature (on-card)
COMPARE	Match input parameter with marker
PIN COMPARE	Match input parameter with marker and limiting number of incorrect compares – reset on successful compare
BIOMETRIC COMPARE	Translate input parameter to template form and compare with base template
SYMMETRIC KEY NONCE	Mutual authenticate of card-application and client-application plus generation of session keys
ANYBODY	NULL authentication protocol

ISO/IEC 24727-4

ISO/IEC 24727 Identification Cards - Integrated circuit cards programming interfaces – Part 4: API administration

- Implementation details of Part 2 and Part 3 interactions
- Normative security architecture and stack configurations
- Normative IFD API
- TLS protocol

Status

- Published

ISO/IEC 24727-5

ISO/IEC 24727 Identification Cards - Integrated circuit cards programming interfaces – Part 5: Testing

Test requirements as technical text is developed

Testing levels and modular approach

Status

- Parts 2, 3, and 4 maturity/stability prerequisite has been met
- Second committee draft ballot – Nov – Dec 2009

Some words about testing

Conformity testing is not easy

- Minimize burden on suppliers
- Consider tendency for broad conformity requests from customers during procurement processes
- Cognizance of testing cost burden
- Flexibility that allows multiple product providers but maintains interoperability goals

ISO/IEC 24727-5

- First attempt yielded unmanageable testing specifications (over 10,000 pages half way through the process)

Refocused testing: Address what is needed to render API

Conformity testing - two phases

- Phase I: Self assertion for initial period of time
- Phase II: Conformity test program

ISO/IEC 24727-6

ISO/IEC 24727 Identification Cards - Integrated circuit cards programming interfaces – Part 6: *Registration authority procedures for the authentication protocols for interoperability*

- Future ISO/IEC 24727 authentication protocols
- Registration of use
- RA streamlines introduction of new normative authentication protocols
- Lead: Standards Australia

Status

Final committee draft Nov-Dec 2009

Summary: ISO/IEC 24727 Identification Cards - Integrated circuit cards programming interfaces

Part 1: *Architecture*

- Framework, common terminology

Part 2: *Generic card interface*

- ISO/IEC 7816 fine-tuning
- Discovery

Part 3: *Application interface*

- Basic services and actions
- Authentication protocols

Part 4: *API administration*

- Security models, stacks
- IFD API

Part 5: *Testing*

Part 6: *Registration authority procedures for the authentication protocols for interoperability*

- Registering future authentication protocols and ISO/IEC 24727 users

Who is using the standard?

Australia

- Australian smartcard framework
- Queensland drivers license – with other AU territories to follow

Europe

- EU Citizen Card (~480M)
- German health card
- German ID card

US

- Consider standard interfaces for future, diverse applications using PIV systems and non-PIV initiatives

Current status

Part 1: *Architecture*

- Published January 2007

Part 2: Generic card interface

- Published **September 2008**

Part 3: Application interface

- Final ballot closed this week, anticipate publication in **November 2008**

Part 4: API administration

- Final ballot passed this month, published **November 2008**

Part 5: Testing

- Initial ballot passed but agreed to launch second committee draft ballot
- Second CD ballot text anticipated in November 2008

Part 6: Registration authority procedures for the authentication protocols for interoperability

- Initial CD passed
- Final committee draft text and ballot in November 2008

Current status

Part 1: *Architecture*

- Published **January 2007**

Part 2: Generic card interface

- Published **September 2008**

With the publication of parts 1, 2, 3, and 4

Part 3: Application interface

- Final ballot closed this week, anticipate publication in **November 2008**

suppliers have a complete specification.

Part 4: API administration

- Final ballot passed this month, publication **November 2008**

Part 5: Testing

It is not perfect but it is ready to apply.

- Initial ballot passed but agreed to launch second committee draft ballot
- Second CD ballot text anticipated in November 2008

Part 6: Registration authority procedures for the authentication protocols for interoperability

- Initial CD passed
- Final committee draft text and ballot in November 2008

Why get involved with standards development?

Developing the US perspective for international bodies is the most important collaborative work for a US TAG

Attendance at national and international meetings brings experts together

Part of the solution, opportunity to influence outcome

More than just a vote – a voice at the table

Further Information

NIST ITL

<http://www.itl.nist.gov/>

NIST ITL Computer Security Resource Center

<http://csrc.nist.gov/>

NIST ITL Biometrics Resource Center

<http://www.nist.gov/biometrics>

Center for Internet Security (CIS)

<http://www.cisecurity.org>

Internet Security Alliance

<http://www.isalliance.org>

Network Reliability and Interoperability Council VI (NRIC VI)

<http://www.nric.org/>

Partnership for Critical Infrastructure Security (PCIS)

<http://www.pcis.org>

Further Information

ISO/IEC JTC 1 (SC 6, SC 17, SC 27, SC 37) <http://www.jtc1.org/>

IETF <http://www.ietf.org>

INCITS (TC B10, M1, T3, T4) <http://www.incits.org/>

X9, Inc. <http://www.x9.org/>

IEEE <http://standards.ieee.org/>

NIST standards.gov web site has an education and training page.

http://standards.gov/standards_gov/educationAndTraining.cfm#section-4

NIST has a 2001 Guide to Documentary Standards

<http://ts.nist.gov/Standards/Conformity/upload/ir6802.pdf>

Teresa.Schwarzhoff@nist.gov

301.975.5727

Thank you.